xSPのルータにおいて設定を推奨するフィルタの項目について（IPv6版）

KDDI 石原 清輝
KDDI 向井 将
DTI 馬渡 将隆

1. アジェンダ

- IRS6 （前回） からのおさらい
  - 主に会場でコメントをいただいた箇所に関して、再度コンセンサスをはかる
- フィルタの項目をジャンル分け
  - 最低限、設定をする事が推奨されるフィルタ
  - （運用者、ルータ）のリソースにより設定を考慮するフィルタ

2. おさらい箇所

- ICMPv6
- Neighbor Discovery
- 6to4
- Long Prefix
- Bogon Prefix
- 6bone

2. おさらい（１）

ICMPv6 について

- 会場で出ていたコメント
  - ICMPv6 の全てを accept する。
  - ICMPv6 の必要な TYPE を選び、それらだけを accept する。
- オペレータのリソースにより対応を考慮する
  - 全てを accept するか？ 必要な TYPE のみを accept するか？
  - Path MTU Discovery が動かない環境にしてはいけない為、全てを reject してしまう事は NG 。

2. おさらい（2）

Neighbor Discovery について

- 会場で出ていたコメント
  - reject していても問題は見られないかもしれないが、将来的には分らない？
    （RA についての話ではそうかも？）
  - 基本的には accept で統一をしてしまっても良いだろう。
- 現時点での対応としては…
  - 基本的には accept で統一をしておく。
    - 文書には Neighbor Discovery の言葉の定義も必要

2. おさらい（3）
6to4について

- 会場で出ていたコメント
  - 公共性について
  - 今後 6to4 自体どのようになっていくのか？
    - すぐになくなると言う事は無いと思われる
    - 実際に活用をしている人はいる
- 現時点での対応としては…
  - フィルタ設定をする場合には、exact match で accept をする。
  - 文書には appendix として情報を書いておく。

2. おさらい（４）

Long Prefix について

- 会場で出ていたコメント
  - /49 or longer を reject するとして良いのか？
  - 文書で明文化をすると問題が出て来ないか？
  - 実際に /48 の prefix は流れているのが現状。

- 現時点での対応としては…
  - /32-/48 の間で accept をする事で良しとする。
  - その中での設定については xSP のポリシー次第。

2. おさらい（5）

Bogon Prefix について

- 会場で出ていたコメント
  - RIR に割り振られた prefix のみ accept？
  - RIR が発行している delegated-latest を元にフィルタを生成？

- 現時点での対応としては…
  - 現状では、フィルタ設定の元とする事が出来るデータが無い。
  - IPv6 IRR を利用する事で対応が出来る？

2. おさらい（6）

6bone について

- 会場で出ていたコメント
  - 2006/06/06 に停止する予定だが、本当に停止するのかどうかは良く分らない？
  - 強制的に reject をした場合、どの程度の影響度なのかも不明。
- 現時点での対応としては…
  - 停止した時以降で、Prefix を reject する程度で考えておけば良い。
  - 文書には appendix として情報を書いておく。

フィルタ項目ジャンル分け

フィルタリングをする箇所

- ピア接続
- トランジット接続
- 顧客接続
- ルーター自身へのアクセス

登場するアドレス

- default
  - ::/0
- ::/8
  - ループバックアドレス
    - ::1/128
  - 未指定アドレス
    - ::/128
  - IPv4互換アドレス
    - ::ffff:/96
  - IPv4射影アドレス
    - ::/96
- リンクローカルアドレス
  - fe80::/10
- サイトローカルアドレス
  - fec0::/10
- ユニークローカルアドレス
  - fec0::/7
- マルチキャストアドレス
  - ff00::/8
- ドキュメントアドレス
  - 2001:db8::/32
- 自ASのprefix
  - まさに2001:db8::/32の出番☺
- 6to4
  - 2002::/16

ピア接続 パケットフィルタリング

- Ingress
  - accept
    - Neighbor Discovery
  - reject
    - source addressが、
      - ::/8　　サイトローカル　ユニークローカル
      - ドキュメント　　マルチキャスト　自ASのprefix
- Egress
  - 特に必要なし

ピア接続 経路フィルタリング

- Ingress
  - prefix-filter
    - accept
      - prefix-length /32～/48
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - 特になし

ピア接続 経路フィルタリング

- Egress
  - prefix-filter
    - accept
      - 自ASのprefixを集約したもの
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - reject
      - private ASN

トランジット接続 パケットフィルタリング

- Ingress
  - accept
    - Neighbor Discovery
  - reject
    - source addressが、
      - ::/8　　サイトローカル　ユニークローカル
      - ドキュメント　　マルチキャスト　自ASのprefix
- Egress
  - 特に必要なし

トランジット接続
経路フィルタリング

- Ingress
  - prefix-filter
    - accept
      - 自ASのprefixを集約したもの
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - 特になし

トランジット接続
経路フィルタリング

- Egress
  - prefix-filter
    - accept
      - 自ASのprefixを集約したもの
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - reject
      - private ASN

顧客接続 パケットフィルタリング

- Ingress
  - accept
    - Neighbor Discovery
  - reject
    - source addressが、
      - ::/8　　サイトローカル　ユニークローカル
      - ドキュメント　　マルチキャスト
  - トランジット顧客の場合
    - reject
      - 自ASのprefixがsource addressのパケット
- Egress
  - 特に必要なし

顧客接続　経路フィルタリング

- Ingress
  - prefix-filter
    - accept(exact)
      - プライベートASを利用したBGP接続の場合、顧客に割り当てたprefix
      - トランジット接続の顧客の場合、顧客側ASからアナウンスされるprefix
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - 特になし

顧客接続　経路フィルタリング

- Egress
  - prefix-filter
    - accept
      - 自ASのprefixを集約したもの
    - reject (exact)
      - default
    - reject (or longer)
      - ::/8　　リンクローカル　サイトローカル
      - ユニークローカル　ドキュメント　　マルチキャスト
      - 自ASのprefix
  - as-path filter
    - reject
      - private ASN

ルータ自身へのアクセス パケットフィルタリング

- Ingress
  - ルータで動かしているサービスのうち、アクセス可能なsource addressを限定してaccept
    - TELNET / SSH / SNMP / FTP/ TFTP / NTP
  - 利用しないサービスはもちろんdisable
  - eBGP / iBGPのneighbor addressのみ179/tcpでaccept
  - 接続リンクにおいて、source addressがリンクローカルのパケットはaccept
    - Neighbor Discoveryもaccept
- Egress
  - 特に必要なし

ピア接続 パケットフィルタリング（リソースに余裕があれば）

- Ingress
  - IX 接続やプライベートピア接続で使用をしているインターフェースでのICMP6の制限
    - 前提条件：Path MTU Discovery (TYPE=2 : Packet too Big)　は、accept する
      - ICMP6 TYPE を制限してaccept
      - 優先度の変更、一定のパケット長を超えたものは reject するなど
- Egress
  - reject
    - source addressが、
      - ::/8　サイトローカル　ユニークローカル
      - ドキュメント　マルチキャスト　自ASのprefix

ピア接続 経路フィルタリング（リソースに余裕があれば）

- Ingress
  - prefix-filter
    - /32～/48はacceptし、/49 or longerはreject
    - ピアの相手からアナウンスされると通知のあったprefixのみaccept
    - 未割り当てのprefixをreject
      - だけど信頼できる情報源が・・・orz
  - as-path filter
    - 一定値以上の長いas-path長の経路をreject
    - ピアの相手からアナウンスされると連絡があったas-pathのみaccept
- Egress
  - 特になし

トランジット接続　パケットフィルタリング (リソースに余裕があれば)

- Ingress
  - トランジット接続で使用をしているインターフェースでのICMP6の制限
    - 前提条件:Path MTU Discovery (TYPE=2 : Packet too Big)　　は、accept する
      - ICMP6 TYPE を制限してaccept
      - 優先度の変更、一定のパケット長を超えたものは reject するなど
- Egress
  - reject
    - source addressが、
      - ::/8　　サイトローカル　ユニークローカル
      - ドキュメント　　マルチキャスト　自ASのprefix

トランジット接続 経路フィルタリング（リソースに余裕があれば）

- Ingress
  - prefix-filter
    - /32～/48はacceptし、/49 or longerはreject
    - ピアの相手からアナウンスされると通知のあったprefixのみaccept
    - 未割り当てのprefixをreject
      - だけど信頼できる情報源が・・・orz
  - as-path filter
    - 一定値以上の長いas-path長の経路をreject
    - ピアの相手からアナウンスされると連絡があったas-pathのみaccept
- Egress
  - 特になし

顧客接続　パケットフィルタリング（リソースに余裕があれば）

- Ingress
  - 顧客接続で使用をしているインターフェースでのICMP6の制限
    - 前提条件：Path MTU Discovery (TYPE=2 : Packet too Big)　　は、accept する
      - ICMP6 TYPE を制限してaccept
      - 優先度の変更、一定のパケット長を超えたものは reject するなど
  - 顧客側で持っているアドレスブロックがsource addressとなっているパケットをaccept
- Egress
  - reject
    - source addressが、
      - ::/8　　サイトローカル　ユニークローカル
      - ドキュメント　　マルチキャスト　自ASのprefix

顧客接続 経路フィルタリング（リソースに余裕があれば）

- Ingress
  - prefix-filter
    - ピアの相手からアナウンスされると通知のあったprefixのみaccept
  - as-path filter
    - ピアの相手からアナウンスされると連絡があったas-pathのみaccept
- Egress
  - 特になし

ルータ自身　パケットフィルタリング (リソースに余裕があれば)

- Ingress
  - ルータでアドレスを設定しているインターフェースでのICMP6の制限
    - 前提条件：Path MTU Discovery (TYPE=2 : Packet too Big)　　は、accept する
      - ICMP6 TYPE を制限してaccept
      - 優先度の変更、一定のパケット長を超えたものは reject するなど
- Egress
  - 特になし
- System Protection ACL
  - RPを保護するため

NTP [janog:06696]

- NTPサーバ(stratum1とか2)はcritical infra?
- パケットフィルタでrejectされるのは厳しい
  - peer / transit / 顧客接続ではacceptする必要あり？
  - 最近のエンドユーザは、microsoftさん、mfeedさんなどが提供するNTPサーバを利用するので、acceptする必要あり？
  - ネットワーク運用側は自前でNTPサーバを立ち上げてますが・・・
  - そもそもIPv4で明示的にacceptしてます？

（参考）Delegated Latest

- RIRが公開している最新の割り振りのリスト[janog:06691]
  - APNIC
    - http://ftp.apnic.net/stats/apnic/delegated-apnic-latest
  - RIPE/NCC
    - ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest
  - ARIN
    - ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest
  - LACNIC
    - ftp://lacnic.net/pub/stats/lacnic/delegated-lacnic-latest
  - AfriNIC
    - ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest